CLARK HILL
Myriah V. Jaworski, Esq., (SBN 336898)
mjaworski@clarkhill.com
555 Flower St., 24th Floor
Los Angeles, CA 90071
Telephone: (619) 557-0404
Facsimile: (619) 557-0460

Attorneys for Defendant
SMITH, GAMBRELL & RUSSELL, LLP

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

CHARLES OWENS AND FELICIA LIVINGSTON as individuals and on behalf of all others similarly situated, Plaintiff, v. SMITH, GAMBRELL & RUSSELL INTERNATIONAL, LLP; AND DOES 1 - 10, Defendant.	Case No. 2:23-cv-01789-JAK-JDE CLASS ACTION **DEFENDANT SMITH, GAMBRELL & RUSSELL, LLP'S ANSWER TO PLAINTIFFS' FIRST AMENDED CLASS ACTION COMPLAINT** Date: August 6, 2024 Judge: Hon. John A. Kronstadt Complaint Filed: Trial Date: None Set

Defendant SMITH, GAMBRELL & RUSSELL, LLP[1] ("Defendant" or "SGR") hereby provides the following Answer to Plaintiffs' First Amended Complaint:

[1] Plaintiffs have named the incorrect entity. SGR, LLP, a Georgia limited liability partnership, operated SGR's U.S. law firm. Smith, Gambrell & Russell International, LLP, is a subsidiary that operates SGR's practice in the United Kingdom.

GENERAL DENIAL

Pursuant to Fed. R. Civ. P. 8(b)(3), unless expressly admitted, Defendants generally and specifically every allegation in Plaintiffs' Complaint, and the whole thereof, including every purported cause of action contained therein and denies that Plaintiffs have been damaged in the sum or sums alleged, or in any other sum or sums, or at all.

ANSWER

I.

SUMMARY OF THE CASE

1. This putative class action arises from Smith, Gambrell & Russell International, LLP's (hereinafter "SGR") negligent failure to implement and maintain reasonable cybersecurity procedures that resulted in a data breach of its systems on or around July 19, 2021 through July 28, 2021, which was discovered on or around August 9, 2021 (the "Data Breach"). In connection with the Data Breach, SGR failed to properly secure and safeguard Plaintiffs' and Class Members' protected personally identifiable information, including without limitation, full names, Social Security numbers and driver's license numbers (these types of information, *inter alia*, being thereafter referred to, collectively, as "personal identifiable information" or "PII").[2] While SGR claims to have discovered the breach in August 2021, the firm did not start informing victims of the Data Breach for nearly a year, and in some instances, approximately 17 months after the breach.

[2] Personally identifiable information ("PII") generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on its face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security numbers, passport numbers, driver's license numbers, financial account numbers).

According to three different notices reported to the Office of the Maine Attorney General, the Data Breach has impacted approximately 104,316 individuals. Plaintiffs bring this class action complaint to redress injuries related to the Data Breach, on behalf of themselves and a nationwide class and California and Georgia subclasses of similarly situated persons. Plaintiffs assert claims on behalf of a nationwide class for negligence, negligence per se, declaratory judgment, common law invasion of privacy, breach of implied contract and breach of implied covenant of good faith and fair dealing. Plaintiffs also brings claims on behalf of a California subclass for violation of the California Consumer Privacy Act, Cal. Civ. Code § 1798.150, the California Customer Records Act, Cal. Civ. Code § 1798.80 *et seq*., violation of the California Unfair Competition Law, Cal. Bus. & Prof. Code § 17200 *et seq*., and for invasion of privacy based on the California Constitution, Art. 1, § 1. Plaintiffs seek, among other things, compensatory damages, punitive and exemplary damages, injunctive relief, attorneys' fees, and costs of suit. Plaintiff Charles Owens further seeks statutory damages on behalf of the California subclass pursuant to Cal. Civ. Code §§ 1798(a)(1)(A)-(C), (a)(2), and (b).

ANSWER: Paragraph 1 violates Fed. R. Civ. P. 8(d)(1) because it is not "simple, concise, and direct". Paragraph 1 also violates Fed. R. Civ. P. 10(b) which requires Plaintiff's Complaint limit its claims "as far as practicable to a single set of circumstances," as Paragraph 1 is a monologue explanation of Plaintiffs' entire Complaint. To the extent that an Answer is required, SGR admits only that it suffered a data security incident from approximately July 19, 2021, to July 28, 2021 (the "Incident"); that SGR learned of the Incident on August 9, 2021; that SGR reported to the Office of the Maine Attorney General that approximately 104,316 individuals were impacted in the Incident as required by that jurisdiction's reporting requirements; and that SGR began notifying

potentially impacted individuals of the Incident on June 28, 2022, SGR denies the remaining allegations contained in Paragraph 1.

II.

PARTIES

2. Plaintiff Charles Owens is a citizen and resident of the State of California whose personal identifying information was part of the July 2021 data breach that is the subject of this action.

ANSWER: SGR lacks knowledge or information sufficient to form a belief as to the truth of the allegations in this paragraph and therefore denies same.

3. Plaintiff Felicia Livingston is a citizen and resident of the State of Georgia whose personal identifying information was part of the July 2021 data breach that is the subject of this action.

ANSWER: SGR lacks knowledge or information sufficient to form a belief as to the truth of the allegations in this paragraph and therefore denies same.

4. On information and belief, Defendant Smith, Gambrell & Russell International, LLP is a law partnership with offices throughout the world, including but not limited to, in Los Angeles, California.

ANSWER: SGR denies the allegations contained within Paragraph 4. SGR affirmatively asserts that Smith, Gambrell, & Russell, LLP is a law partnership with offices throughout the world, including but not limited to, in Los Angeles, California. Smith, Gambrell, & Russell International, LLP is a subsidiary that operates in the United Kingdom.

5. Plaintiffs bring this action on behalf of themselves, on behalf of the general public as a Private Attorney General pursuant to California Code of Civil Procedure § 1021.5 and on behalf of a class and subclass of similarly situated persons pursuant Federal Rule of Civil Procedure 23.

ANSWER: Paragraph 5 states a legal conclusion and does not contain a factual allegation to which an admission or denial is required. To the extent that an answer is required, SGR denies the allegations contained in Paragraph 5.

III.

JURISDICTION & VENUE

6. This Court has general personal jurisdiction over SGR because, at all relevant times, the company had systematic and continuous contacts with the State of California. SGR does business in California and has offices in Los Angeles, California. Defendant regularly contracts with a multitude of businesses, organizations and consumers in California to provide legal services. SGR does in fact actually provide such continuous and ongoing legal services to such customers in California and has employees in California.

ANSWER: Paragraph 6 contains a legal conclusion to which no answer is required. To the extent that an answer is required, SGR admits that this Court maintains personal jurisdiction over it.

7. Furthermore, this Court has specific personal jurisdiction over SGR because the claims in this action stem from its specific contacts with the State of California — namely, SGR's provision of legal services to a multitude of clients in California, SGR's collection, maintenance, and processing of the personal data of Californians in connection with such services, including but not limited to SGR's employees, SGR's failure to implement and maintain reasonable security procedures and practices with respect to that data, and the consequent cybersecurity attack and security breach of such data in July 2021.

ANSWER: Paragraph 7 contains a legal conclusion to which no answer is required. To the extent that an answer is required, SGR admits only that it provides legal services in California, and denies the remaining allegations contained in Paragraph 7.

8. This Court has diversity subject matter jurisdiction under 28 U.S.C. § 1332(d) in that the mater in controversy exceeds the sum or value of $5,000,000, exclusive of interests and costs, and is a class action in which members of the class defined herein include citizens of a State different from the SGR.

ANSWER: Paragraph 8 contains a legal conclusion to which no answer is required. To the extent that an answer is required, SGR denies the allegations contained in Paragraph 8.

9. Supplemental jurisdiction to adjudicate issues pertaining to state law is proper in this Court pursuant to 28 U.S.C. § 1367.

ANSWER: Paragraph 9 contains a legal conclusion to which no answer is required. To the extent that an answer is required, SGR denies the allegations contained in Paragraph 9.

10. Venue is proper in the Central District of California under 28 U.S.C. § 1391 (b)(1)-(2) and (c)(2) because a substantial part of the events or omissions giving rise to the claims alleged herein occurred within this judicial district, specifically SGR's provision of legal services in California and within Los Angeles County, SGR's collection, maintenance, and processing of the personal data of Californians in connection with such services, SGR's failure to implement and maintain reasonable security procedures and practices with respect to that data, and the consequent security breach of such data in July 2021 that resulted from SGR's failure. In addition, Plaintiffs are informed and believe and thereon allege that members of the class and subclass defined below reside in the Central District, and SGR has offices within the Central District.

ANSWER: Paragraph 10 contains a legal conclusion to which no answer is required. To the extent that an answer is required, SGR admits only that it provides legal services in California and Los Angeles County, and denies the remaining allegations contained in Paragraph 10.

IV.

FACTUAL BACKGROUND

11. SGR is an international law firm with more than 400 lawyers operating in 14 domestic and international offices.

ANSWER: SGR admits that it is an international law firm operating in 11 domestic and international offices. SGR denies the remaining allegations contained in Paragraph 11.

12. In connection with its law practice, SGR collects, stores, and processes sensitive personal data for thousands of individuals, including but not limited to its clients and employees. In doing so, SGR retains sensitive information including, but not limited to, bank account information, health care related information, addresses, driver's license numbers, and social security numbers, among other things.

ANSWER: SGR denies that it "processes" sensitive personal data. SGR admits only that it collects and stores data for individuals. The allegation that some information was sensitive is a legal conclusion to which no response is required. SGR denies the remaining allegations in Paragraph 12.

13. As a law partnership doing business in California and having employees and clients in California, SGR is legally required to protect personal information from unauthorized access, disclosure, theft, exfiltration, modification, use, or destruction.

ANSWER: Paragraph 13 contains an incorrect recitation of Customer Records (Cal. Civil Code §§ 1798.80–1798.84), which actually states that a business "implement and maintain reasonable security procedures and practices appropriate to the nature of the information, [and] to protect the personal information [of its customers] from unauthorized access, destruction, use, modification, or disclosure." Plaintiffs are not customers of SGR and therefore

the Customer Records Act does not apply. Answering further, SGR denies the allegations contained within Paragraph 13.

14. SGR knew that it was a prime target for hackers given the significant amount of sensitive personal information processed through its computer data and storage systems. SGR's knowledge is underscored by the massive number of data breaches that have occurred in recent years.

ANSWER: SGR denies the allegations contained in Paragraph 14.

15. Despite knowing the prevalence of data breaches, SGR failed to prioritize data security by adopting reasonable data security measures to prevent and detect unauthorized access to its highly sensitive systems and databases. SGR has the resources to prevent a breach, but neglected to adequately invest in data security, despite the growing number of well-publicized breaches. SGR failed to undertake adequate analyses and testing of its own systems, training of its own personnel, and other data security measures as described herein to ensure vulnerabilities were avoided or remedied and that Plaintiffs' and Class Members' data were protected.

ANSWER: SGR denies the allegations contained in Paragraph 15.

16. Specifically, on or around August 9, 2021, SGR discovered a significant cybersecurity breach. SGR's subsequent investigation revealed that a number of documents may have been taken from SGR's files and information technology systems during the period July 19, 2021 through July 28, 2021.

ANSWER: SGR admits that it discovered the Incident on August 9, 2021. SGR denies the remaining allegations contained in Paragraph 16.

17. On information and belief, the personal information SGR collects and which was impacted by the cybersecurity attack includes individuals' name, social security number, driver's license number, non-driver identification number, and health information such as medical history, treatment and diagnosis, among other personal, sensitive and confidential information.

ANSWER: SGR admits only information which may have been impacted in the Incident includes for some individuals at least one of: name, social security number, driver's license number, non-driver identification number, and health information such as medical history, treatment, and diagnosis. SGR denies the remaining allegations contained in Paragraph 17.

18. SGR reported three separate data breach notices regarding the 2021 data breach to the Office of the Maine Attorney General. The first notice, which was reported on June 28, 2022, indicated that 6,515 persons were affected by the data breach. The second notice, which was reported on August 8, 2022, indicated that 19,322 persons were affected by the data breach. The most recent notice, which was reported on March 1, 2023, indicated that 78,479 persons were affected by the data breach. In total, SGR has indicated that approximately 104,316 individuals were impacted by the 2021 data breach.[3]

ANSWER: SGR admits that it reported to the Office of the Maine Attorney General in three separate communications that 104,316 individuals were impacted by the Incident as required by Maine.

19. SGR waited more than 17 months to notify some impacted individuals of the breach. Between December 13, 2022 and January 13, 2023, SGR mailed data breach notices to latest batch of impacted parties. According to notice mailed to impacted individuals, the breach resulted in individuals' name, social security number, driver's license number, non-driver identification number, and health information such as medical history, treatment and diagnosis, being compromised and acquired by unauthorized actors. Plaintiffs received a copy of the January 13,

[3] Data Breach Notifications, https://apps.web.maine.gov/online/aeviewer/ME/40/list.shtml (last accessed June 27, 2023).

2023 data breach notice via United States mail service confirming that their personal identifying information was part of the data breach.

ANSWER: SGR admits only that it notified a group of potentially impacted individuals of the Incident between December 13, 2022, and January 13, 2023. SGR denies the remaining allegations contained in Paragraph 19.

20. Upon information and belief, the hackers responsible for the Data Breach stole the personal information many of SGR's clients and employees, including Plaintiffs'. Because of the nature of the breach and of the personal information stored or processed by SGR, Plaintiff is informed and believes that all categories of personal information were further subject to unauthorized access, disclosure, theft, exfiltration, modification, use, or destruction. Plaintiffs are informed and believes that criminals would have no purpose for hacking SGR other than to exfiltrate or steal, or destroy, use, or modify as part of their ransom attempts, the coveted personal information stored or processed by SGR.

ANSWER: SGR denies the allegations contained within Paragraph 20.

21. The personal information exposed by SGR as a result of its inadequate data security is highly valuable on the black market to phishers, hackers, identity thieves, and cybercriminals. Stolen personal information is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines. Law enforcement has difficulty policing the dark web due to this encryption, which allows users and criminals to conceal identities and online activity.

ANSWER: SGR denies engaging in any inadequate practices or that its practices caused the Incident. Answering further, the remaining allegations in Paragraph 21 are irrelevant because Plaintiffs have not alleged that they have found their information on the dark web and paragraph 21 merely speculates to future events that may or may not ever occur. To the extent that an answer

is required, SGR lacks knowledge or information sufficient to form a belief as to the truth of the allegations in this paragraph and therefore denies same.

22. When malicious actors infiltrate companies and copy and exfiltrate the personal information that those companies store, or have access to, that stolen information often ends up on the dark web because the malicious actors buy and sell that information for profit.

ANSWER: Paragraph 22 does not contain allegations related to the Incident or any facts or events that Plaintiffs allege occurred as a result of the Incident and merely speculates to future events that may or may not ever occur; therefore, an answer is not required. To the extent that an answer is required, SGR lacks knowledge or information sufficient to form a belief as to the truth of the allegations in this paragraph and therefore denies same.

23. The information compromised in this unauthorized cybersecurity attack involves sensitive personal identifying information, which is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. Whereas here, the information compromised is difficult and highly problematic to change—particularly social security numbers.

ANSWER: Paragraph 23 does not contain allegations related to the Incident or any facts or events that Plaintiffs allege occurred as a result of the Incident and merely speculates to future events that may or may not ever occur; therefore, an answer is not required. To the extent that an answer is required, SGR lacks knowledge or information sufficient to form a belief as to the truth of the allegations in this paragraph and therefore denies the same.

24. Once personal information is sold, it is often used to gain access to various areas of the victim's digital life, including bank accounts, social media, credit card, and tax details. This can lead to additional personal information being

harvested from the victim, as well as personal information from family, friends, and colleagues of the original victim.

ANSWER: Paragraph 24 does not contain allegations related to the Incident or any facts or events that Plaintiffs allege occurred as a result of the Incident and merely speculates to future events that may or may not ever occur; therefore, an answer is not required. To the extent that an answer is required, SGR lacks knowledge or information sufficient to form a belief as to the truth of the allegations in this paragraph and therefore denies same.

25. Unauthorized data breaches, such as these, facilitate identity theft as hackers obtain consumers' personal information and thereafter use it to siphon money from current accounts, open new accounts in the names of their victims, or sell consumers' personal information to others who do the same.

ANSWER: Paragraph 25 does not contain allegations related to the Incident or any facts or events that Plaintiffs allege occurred as a result of the Incident and merely speculates to future events that may or may not ever occur; therefore, an answer is not required. To the extent that an answer is required, SGR lacks knowledge or information sufficient to form a belief as to the truth of the allegations in this paragraph and therefore denies same.

26. The high value of PII to criminals is further evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[4] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on

[4] *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the- dark-web-how-much-it-costs/ (last accessed July 28, 2021)

the dark web.[5] Criminals can also purchase access to entire company data breaches from $999 to $4,995.[6]

ANSWER: Paragraph 26 does not contain allegations related to the Incident or any facts or events that Plaintiffs allege occurred as a result of the Incident and merely speculates to future events that may or may not ever occur; therefore, an answer is not required. To the extent that an answer is required, SGR lacks knowledge or information sufficient to form a belief as to the truth of the allegations in this paragraph and therefore denies same.

27. These criminal activities have and will result in devastating financial and personal losses to Plaintiffs and Class Members. For example, it is believed that certain PII compromised in the 2017 Experian data breach was being used, three years later, by identity thieves to apply for COVID-19-related benefits in the state of Oklahoma. Such fraud will be an omnipresent threat for Representative Plaintiffs and Class Members for the rest of their lives. They will need to remain constantly vigilant.

ANSWER: Paragraph 27 does not contain allegations related to the Incident or any facts or events that Plaintiffs allege occurred as a result of the Incident and merely speculates to future events that may or may not ever occur; therefore, an answer is not required. To the extent that an answer is required, SGR lacks knowledge or information sufficient to form a belief as to the truth of the allegations in this paragraph and therefore denies same.

---

[5] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed November 5, 2021).

[6] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed January 21, 2022).

28. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."

ANSWER: Paragraph 28 does not contain allegations related to the Incident or any facts or events that Plaintiffs allege occurred as a result of the Incident; therefore, an answer is not required. To the extent that an answer is required, SGR lacks knowledge or information sufficient to form a belief as to the truth of the allegations in this paragraph and therefore denies same.

29. Identity thieves can use PII, such as that of Plaintiffs and Class Members which SGR failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, using the victim's information to obtain government benefits, or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

ANSWER: Paragraph 29 does not contain allegations related to the Incident or any facts or events that Plaintiffs allege occurred as a result of the Incident and merely speculates to future events that may or may not ever occur; therefore, an answer is not required. To the extent that an answer is required, SGR lacks knowledge or information sufficient to form a belief as to the truth of the allegations in this paragraph and therefore denies same.

30. The ramifications of SGR's failure to keep secure Plaintiffs' and Class Members' PII are long lasting and severe. Once PII is stolen, particularly

identification numbers, fraudulent use of that information and damage to victims may continue for years. Indeed, Plaintiffs' and Class Members' PII was taken by hackers to engage in identity theft or to sell it to other criminals who will purchase the PII for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

ANSWER: Paragraph 30 does not contain allegations related to the Incident or any facts or events that Plaintiffs allege occurred as a result of the Incident and merely speculates to future events that may or may not ever occur; therefore, an answer is not required. To the extent that an answer is required, SGR lacks knowledge or information sufficient to form a belief as to the truth of the allegations in this paragraph and therefore denies same.

31. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[7]

ANSWER: Paragraph 31 does not contain allegations related to the Incident or any facts or events that Plaintiffs allege occurred as a result of the Incident and merely speculates to future events that may or may not ever occur; therefore, an answer is not required. To the extent that an answer is required, SGR lacks

[7] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* http://www.gao.gov/new.items/d07737.pdf (last accessed January 21, 2022).

knowledge or information sufficient to form a belief as to the truth of the allegations in this paragraph and therefore denies same.

32. When cyber criminals access financial information and other personally sensitive data—as they did here—there is no limit to the amount of fraud to which Defendant may have exposed Plaintiffs and Class Members.

ANSWER: SGR denies the allegations contained in Paragraph 32.

33. And data breaches are preventable.[8] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "[i]n almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[9] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[10]

ANSWER: Paragraph 33 does not contain allegations related to the Incident or any facts or events that Plaintiffs allege occurred as a result of the Incident; therefore, an answer is not required. To the extent that an answer is required, SGR lacks knowledge or information sufficient to form a belief as to the truth of the allegations in this paragraph and therefore denies same.

34. Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures ... Appropriate information security controls, including encryption, must be

[8] Lucy L. Thompson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012)

[9] *Id.* at 17.

[10] *Id.* at 28.

implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*.[11]

ANSWER: Paragraph 34 does not contain allegations related to the Incident or any facts or events that Plaintiffs allege occurred as a result of the Incident; therefore, an answer is not required. To the extent that an answer is required, SGR lacks knowledge or information sufficient to form a belief as to the truth of the allegations in this paragraph and therefore denies same.

35. Federal and state governments have established security standards and issued recommendations to minimize unauthorized data disclosures and the resulting harm to individuals and financial institutions. Indeed, the Federal Trade Commission ("FTC") has issued numerous guides for businesses that highlight the importance of reasonable data security practices.

ANSWER: Paragraph 35 does not contain allegations related to the Incident or any facts or events that Plaintiffs allege occurred as a result of the Incident; therefore, an answer is not required. To the extent that an answer is required, SGR lacks knowledge or information sufficient to form a belief as to the truth of the allegations in this paragraph and therefore denies same.

36. According to the FTC, the need for data security should be factored into all business decision-making.[12] In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business.[13] Among other

---

[11] *Id*.

[12] *See* Federal Trade Commission, Start with Security (June 2015), available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited February 3, 2023).

[13] *See* Federal Trade Commission, Protecting Personal Information: A Guide for Business (Oct. 2016), available at

things, the guidelines note businesses should properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of the breach.

ANSWER: Paragraph 36 does not contain allegations related to the Incident or any facts or events that Plaintiffs allege occurred as a result of the Incident; therefore, an answer is not required. To the extent that an answer is required, SGR lacks knowledge or information sufficient to form a belief as to the truth of the allegations in this paragraph and therefore denies same.

37. Also, the FTC recommends that companies limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures.[14]

ANSWER: Paragraph 37 does not contain allegations related to the Incident or any facts or events that Plaintiffs allege occurred as a result of the Incident; therefore, an answer is not required. To the extent that an answer is required, SGR lacks knowledge or information sufficient to form a belief as to the truth of the allegations in this paragraph and therefore denies same.

38. Highlighting the importance of protecting against unauthorized data disclosures, the FTC has brought enforcement actions against businesses for failing

---

https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited February 3, 2023).

[14] *See id*.

to adequately and reasonably protect personal information, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45.

ANSWER: Paragraph 38 does not contain allegations related to the Incident or any facts or events that Plaintiffs allege occurred as a result of the Incident; therefore, an answer is not required. To the extent that an answer is required, SGR lacks knowledge or information sufficient to form a belief as to the truth of the allegations in this paragraph and therefore denies same.

39. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

ANSWER: Paragraph 39 does not contain allegations related to the Incident or any facts or events that Plaintiffs allege occurred as a result of the Incident; therefore, an answer is not required. To the extent that an answer is required, SGR lacks knowledge or information sufficient to form a belief as to the truth of the allegations in this paragraph and therefore denies same.

40. The FBI created a technical guidance document for Chief Information Officers and Chief Information Security Officers that compiles already existing federal government and private industry best practices and mitigation strategies to prevent and respond to ransomware attacks. The document is titled *How to Protect Your Networks from Ransomware* and states that on average, more than 4,000 ransomware attacks have occurred daily since January 1, 2016. Yet, there are very effective prevention and response actions that can significantly mitigate the risks.[15] Preventative measure include:

[15] *How to Protect Your Networks from Ransomware*, FBI, https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last viewed February 3, 2023).

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used. Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[16]

ANSWER: Paragraph 40 does not contain allegations related to the Incident or any facts or events that Plaintiffs allege occurred as a result of the Incident; therefore, an answer is not required. To the extent that an answer is required,

[16] *Id.*

SGR lacks knowledge or information sufficient to form a belief as to the truth of the allegations in this paragraph and therefore denies same.

41. SGR could have prevented the cybersecurity attack by properly utilizing best practices as advised by the federal government, as described in the preceding paragraphs, but failed to do so.

ANSWER: SGR denies the allegations contained in Paragraph 41.

42. SGR's failure to safeguard against a cybersecurity attack is exacerbated by the repeated warnings and alerts from public and private institutions, including the federal government, directed to protecting and securing sensitive data. Experts studying cybersecurity routinely identify companies such as SGR that collect, process, and store massive amounts of data on cloud-based systems as being particularly vulnerable to cyberattacks because of the value of the personal information that they collect and maintain. Accordingly, SGR knew or should have known that it was a prime target for hackers.

ANSWER: SGR denies the allegations contained in Paragraph 42.

43. According to the 2021 Thales Global Cloud Security Study, more than 40% of organizations experienced a cloud-based data breach in the previous 12 months. Yet, despite these incidents, the study found that nearly 83% of cloud-based businesses still fail to encrypt half of the sensitive data they store in the cloud.[17]

ANSWER: Paragraph 43 does not contain allegations related to the Incident or any facts or events that Plaintiffs allege occurred as a result of the Incident; therefore, an answer is not required. To the extent that an answer is required, SGR lacks knowledge or information sufficient to form a belief as to the truth of the allegations in this paragraph and therefore denies same.

[17] Maria Henriquez, *40% of organizations have suffered a cloud-based data breach,* Security, Oct. 29, 2021, https://www.securitymagazine.com/articles/96412-40-of-organizations-have-suffered-a-cloud-based-datq-breach (last visited February 3, 2023).

44. Upon information and belief, SGR did not encrypt Plaintiffs' and Class Members' personal information involved in the data breach.

ANSWER: SGR denies the allegations in Paragraph 44.

45. Despite knowing the prevalence of data breaches, SGR failed to prioritize cybersecurity by adopting reasonable security measures to prevent and detect unauthorized access to its highly sensitive systems and databases. SGR has the resources to prevent an attack, but neglected to adequately invest in cybersecurity, despite the growing number of well-publicized breaches. SGR failed to fully implement each and all of the above-described data security best practices. SGR further failed to undertake adequate analyses and testing of its own systems, training of its own personnel, and other data security measures to ensure vulnerabilities were avoided or remedied and that Plaintiffs' and Class Members' data were protected.

ANSWER: SGR denies the allegations in Paragraph 45.

46. As detailed above, SGR is a large, sophisticated law firm with the resources to deploy robust cybersecurity protocols. It knew, or should have known, that the development and use of such protocols were necessary to fulfill its statutory and common law duties to Plaintiffs and Class Members. Its failure to do so is, therefore, intentional, willful, reckless and/or grossly negligent.

ANSWER: SGR admits that it is a law firm with the resources to deploy cybersecurity protocols. SGR denies the remaining allegations contained in Paragraph 46.

47. SGR disregarded the rights of Plaintiffs and Class Members by, *inter alia*, (i) intentionally, willfully, recklessly, and/or negligently failing to take adequate and reasonable measures to ensure that its network servers were protected against unauthorized intrusions; (ii) failing to disclose that it did not have adequately robust security protocols and training practices in place to adequately safeguard

Plaintiffs' and Class Members' PII; (iii) failing to take standard and reasonably available steps to prevent the Data Breach; (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (v) failing to provide Plaintiffs and Class Members prompt and accurate notice of the Data Breach.

ANSWER: SGR denies the allegations contained within Paragraph 47.

Plaintiff Owens' Facts

48. SGR received highly sensitive personal, health related and financial information from Plaintiff Owens in connection with his employment with Aaron's, LLC. Aaron's, LLC was a client of SGR, and therefore, in possession, custody and/or control of Plaintiff Owens' PII. As a result, Plaintiff Owens' information was among the data accessed by an unauthorized third party in the Data Breach.

ANSWER: SGR admits that Plaintiff Owens' name, social security number and health information such as medical history, treatment and diagnosis were among the data potentially impacted in the Incident. SGR denies the remaining allegations in paragraph 49.

49. At all times herein relevant, Plaintiff Owens is and was a member of the nationwide class and the California subclasses alleged herein.

ANSWER: Paragraph 49 makes an allegation as to a class that does not exist; therefore, SGR denies the allegations contained in Paragraph 49.

50. Plaintiff Owens' PII was exposed in the Data Breach because SGR stored and/or controlled Plaintiffs' PII. Plaintiff Owen's PII was within the possession and control of SGR at the time of the Data Breach.

ANSWER: SGR admits that some of Plaintiff's Owens' PII was within SGR's possession at the time of the Incident. SGR denies the remaining allegations contained within Paragraph 50.

51. Plaintiff Owens received a letter from Defendant, dated January 13, 2023, stating that his name, social security number, and health information such as

medical history, treatment and diagnosis, that was in the possession, custody and/or control of SGR was involved in the Data Breach (the "Notice").

ANSWER: SGR denies the allegations contained in Paragraph 61. SGR admits that it sent Plaintiff Owens a letter dated December 13, 2023, which stated that "some of [Owen's] personal information was contained in potentially impacted documents" including "name, social security number and health information such as medical history, treatment and diagnosis."

52. As a result, Plaintiff Owens spent time dealing with the consequences of the Data Breach, which included and continues to include, time spent verifying the legitimacy and impact of the Data Breach, exploring credit monitoring and identity theft insurance options, self-monitoring his accounts and seeking legal counsel regarding his options for remedying and/or mitigating the effects of the Data Breach. This time has been lost forever and cannot be recaptured.

ANSWER: SGR lacks knowledge or information sufficient to form a belief as to the truth of the allegations in this paragraph and therefore denies same.

53. Plaintiff Owens suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that he entrusted to SGR, which was compromised in and as a result of the Data Breach.

ANSWER: SGR denies the allegations contained within Paragraph 53.

54. Plaintiff Owens suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using, and selling his PII, health information, and/or financial information.

ANSWER: SGR lacks knowledge or information sufficient to form a belief as to the truth of the allegations in this paragraph and therefore denies same.

55. Plaintiff Owens has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII, in combination with his name, being placed in the hands of unauthorized third parties/criminals.

ANSWER: SGR denies the allegations contained within Paragraph 55.

56. Plaintiff Owens has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in SGR's possession, is protected and safeguarded from future breaches.

ANSWER: SGR lacks knowledge or information sufficient to form a belief as to the truth of the allegations in this paragraph and therefore denies same.

Plaintiff Livingston's Facts

57. SGR received highly sensitive personal and financial information from Plaintiff Livingston in connection with goods she purchased from Aaron's, LLC. Aaron's, LLC was a client of SGR, and therefore, in possession, custody and/or control of Plaintiff Livingston's PII. As a result, Plaintiff Livingston's information was among the data accessed by an unauthorized third party in the Data Breach.

ANSWER: SGR admits that it possessed some of Livingston's PII and that it may have been impacted in the Incident. SGR denies the remaining allegations contained within Paragraph 57.

58. Plaintiff Livingston received services—and was a "consumer" for purposes of obtaining services from Aarons, LLC—within the state of Georgia.

ANSWER: SGR lacks knowledge or information sufficient to form a belief as to the truth of the allegations in this paragraph and therefore denies same.

59. At all times herein relevant, Plaintiff Livingston is and was a member of each of the nationwide class and Georgia subclass.

ANSWER: Paragraph 59 makes an allegation as to a class that does not exist; therefore, SGR denies the allegations contained in Paragraph 59.

60. Plaintiff Livingston's PII was exposed in the Data Breach because SGR stored and/or controlled her PII. Plaintiff Livingston's PII was within the possession and control of SGR at the time of the Data Breach.

ANSWER: SGR admits that some of Plaintiff's Livingston's PII was within SGR's possession at the time of the Incident. SGR denies the remaining allegations contained within Paragraph 60.

61. Plaintiff Livingston received a letter from Defendant, dated January 13, 2023, stating that her PII was involved in the Data Breach (the "Notice").

ANSWER: SGR denies the allegations contained in Paragraph 61. SGR admits that it sent Plaintiff Livingston a letter dated January 13, 2023, which stated that "some of [Livingston's] personal information was contained in potentially impacted documents" including "name, social security number, and driver's license number."

62. As a result, Plaintiff Livingston spent time dealing with the consequences of the Data Breach, which included and continues to include, time spent verifying the legitimacy and impact of the Data Breach, exploring credit monitoring and identity theft insurance options, self-monitoring her accounts and seeking legal counsel regarding her options for remedying and/or mitigating the effects of the Data Breach. This time has been lost forever and cannot be recaptured.

ANSWER: SGR lacks knowledge or information sufficient to form a belief as to the truth of the allegations in this paragraph and therefore denies same.

63. Plaintiff Livingston suffered actual injury in the form of damages to and diminution in the value of her PII—a form of intangible property that she entrusted to SGR, which was compromised in and as a result of the Data Breach.

ANSWER: SGR denies the allegations contained within Paragraph 63.

64. Plaintiff Livingston suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns

for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using, and selling her PII.

ANSWER: SGR lacks knowledge or information sufficient to form a belief as to the truth of the allegations in this paragraph and therefore denies same.

65. Plaintiff Livingston has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII, in combination with her name, being placed in the hands of unauthorized third parties/criminals.

ANSWER: SGR denies the allegations contained in Paragraph 65 of Plaintiff's Complaint.

66. Plaintiff Livingston has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in SGR's possession, is protected and safeguarded from future breaches.

ANSWER: SGR lacks knowledge or information sufficient to form a belief as to the truth of the allegations in this paragraph and therefore denies same.

67. Plaintiffs' and Class Members' personal identifying information, including their names, social security numbers, and health information such as medical history, treatment and diagnosis, were in the possession, custody and/or control of SGR. Plaintiffs believed that SGR would protect and keep their personal identifying information protected, secure and safe from unlawful disclosure.

ANSWER: SGR admits only that it stored data of Plaintiffs and other individuals. The allegation that some information was personal identifying information is a legal conclusion to which no response is required. SGR lacks knowledge or information sufficient to form a belief as to the truth of the remaining allegations in this paragraph and therefore denies same.

68. Plaintiffs and Class Members have spent and will continue to spend time and effort monitoring his accounts to protect themselves from identity theft.

Plaintiffs and Class Members remain concerned for their personal security and the uncertainty of what personal information was exposed to hackers and/or posted to the dark web.

ANSWER: SGR lacks knowledge or information sufficient to form a belief as to the truth of the allegations in this paragraph and therefore denies same.

69. As a direct and foreseeable result of SGR's negligent failure to implement and maintain reasonable data security procedures and practices and the resultant breach of its systems, Plaintiffs and all Class Members, have suffered harm in that their sensitive personal information has been exposed to cybercriminals and they have an increased stress, risk, and fear of identity theft and fraud. This is not just a generalized anxiety of possible identify theft, privacy, or fraud concerns, but a concrete stress and risk of harm resulting from an actual breach and accompanied by actual instances of reported problems suspected to stem from the breach.

ANSWER: SGR denies the allegations contained in Paragraph 69.

70. Plaintiffs and Class Members are especially concerned about the misappropriation of their Social Security numbers. Social security numbers are among the most sensitive kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's social security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your

> Social Security number and assuming your identity can cause a lot of problems.[18]

ANSWER: SGR lacks knowledge or information sufficient to form a belief as to the truth of the allegations in this paragraph and therefore denies same. The quote from and citation to the Social Security Administration's website does not require an answer from SGR.

71. Furthermore, Plaintiffs and Class Members are well aware that their sensitive personal information, including social security numbers and potentially banking information, risks being available to other cybercriminals on the dark web. Accordingly, all Plaintiffs and Class Members have suffered harm in the form of increased stress, fear, and risk of identity theft and fraud resulting from the data breach. Additionally, Plaintiffs and Class Members have incurred, and/or will incur, out-of-pocket expenses related to credit monitoring and identify theft prevention to address these concerns.

ANSWER: SGR lacks knowledge or information sufficient to form a belief as to the truth of the allegations in this paragraph and therefore denies same.

CLASS ACTION ALLEGATIONS

72. Plaintiffs bring this action on behalf of themselves and all other similarly situated persons pursuant to Federal Rule of Civil Procedure 23, including Rule 23(b)(1)-(3) and (c)(4). Plaintiffs seek to represent the following class and subclasses:

> **Nationwide Class**. All persons in the United States whose personal information was compromised in or as a result of SGR's data breach discovered by SGR on or around August 9, 2021.

[18] *Identify Theft and Your Social Security Number*, Social Security Administration, https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited February 3, 2023).

> **California Subclass**. All persons residing in California whose personal information was compromised in or as a result of SGR's data breach discovered by SGR on or around August 9, 2021.
>
> **Georgia Subclass**. All persons residing in Georgia whose personal information was compromised in or as a result of SGR's data breach discovered by SGR on or around August 9, 2021.

Excluded from the class are the following individuals and/or entities: SGR and its parents, subsidiaries, affiliates, officers, directors, or employees, and any entity in which SGR has a controlling interest; all individuals who make a timely request to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

ANSWER: The allegations in Paragraph 72 consist of legal conclusions and Plaintiffs' characterizations of their claims and terminology to which no response is required. To the extent that a further response to the allegations contained in Paragraph 72 is required, SGR denies same, denies that it is appropriate for Plaintiffs to bring claims on behalf of the purported Nationwide, California, and Georgia Classes, and denies that such classes may be certified under Rule 23 of the Federal Rules of Civil Procedure.

73. Plaintiffs reserve the right to amend or modify the class definitions with greater particularity or further division into subclasses or limitation to particular issues.

ANSWER: Paragraph 73 lacks any allegations and is merely an attempted reservation of rights to which no response is required. To the extent that a further response in required, SGR denies the allegations contained within Paragraph 73.

74. This action has been brought and may be maintained as a class action under Rule 23 because there is a well-defined community of interest in the litigation and the proposed classes are ascertainable, as described further below:

a. Numerosity: The potential members of the class as defined are so numerous that joinder of all members of the class is impracticable. While the precise number of Class Members at issue has not been determined, Plaintiff believes the cybersecurity breach affected tens of thousands of individuals nationwide and at least many thousands within California.

b. Commonality: There are questions of law and fact common to Plaintiffs and the class that predominate over any questions affecting only the individual members of the class. The common questions of law and fact include, but are not limited to, the following:

i. Whether SGR owed a duty to Plaintiffs and Class Members to exercise due care in collecting, storing, processing, and safeguarding their personal information;

ii. Whether SGR breached those duties;

iii. Whether SGR implemented and maintained reasonable security procedures and practices appropriate to the nature of the personal information of Class Members;

iv. Whether SGR acted negligently in connection with the monitoring and/or protecting of Plaintiffs' and Class Members' personal information;

v. Whether SGR knew or should have known that they did not employ reasonable measures to keep Plaintiffs' and

Class Members' personal information secure and prevent loss or misuse of that personal information;

vi. Whether SGR adequately addressed and fixed the vulnerabilities which permitted the data breach to occur;

vii. Whether SGR caused Plaintiffs and Class Members damages;

viii. Whether the damages SGR caused to Plaintiffs and Class Members includes the increased risk and fear of identity theft and fraud resulting from the access and exfiltration, theft, or disclosure of their personal information;

ix. Whether Plaintiffs and Class Members are entitled to credit monitoring and other monetary relief;

x. Whether SGR's failure to implement and maintain reasonable security procedures and practices constitutes negligence;

xi. Whether SGR's failure to implement and maintain reasonable security procedures and practices constitutes negligence per se;

xii. Whether SGR's failure to implement and maintain reasonable security procedures and practices constitutes violation of the Federal Trade Commission Act, 15 U.S.C. § 45(a);

xiii. Whether SGR's failure to implement and maintain reasonable security procedures and practices constitutes violation of the California Consumer Privacy Act, Cal. Civ. Code § 1798.150, California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200; and

xiv. Whether the California subclass is entitled to actual pecuniary damages under the private rights of action in the California Customer Records Act, Cal. Civ. Code § 1798.84 and the California Consumer Privacy Act, Civ. Code § 1798.150, and the proper measure of such damages, and/or statutory damages pursuant § 1798.150(a)(1)(A) and the proper measure of such damages.

c. Typicality. The claims of the named Plaintiffs are typical of the claims of the Class Members because all had their personal information compromised as a result of SGR's failure to implement and maintain reasonable security measures and the consequent data breach.

d. Adequacy of Representation. Plaintiffs will fairly and adequately represent the interests of the class. Counsel who represent Plaintiffs are experienced and competent in consumer and employment class actions, as well as various other types of complex and class litigation.

e. Superiority and Manageability. A class action is superior to other available means for the fair and efficient adjudication of this controversy. Individual joinder of all Plaintiffs is not practicable, and questions of law and fact common to Plaintiffs predominate over any questions affecting only Plaintiff. Each Plaintiff has been damaged and is entitled to recovery by reason of SGR's unlawful failure to adequately safeguard their data. Class action treatment will allow those similarly situated persons to litigate their claims in the manner that is most efficient and economical

for the parties and the judicial system. As any civil penalty awarded to any individual class member may be small, the expense and burden of individual litigation make it impracticable for most Class Members to seek redress individually. It is also unlikely that any individual consumer would bring an action solely on behalf of himself or herself pursuant to the theories asserted herein. Additionally, the proper measure of civil penalties for each wrongful act will be answered in a consistent and uniform manner. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action, as SGR's records will readily enable the Court and parties to ascertain affected companies and their employees.

f. Notice to Class. Among other means, potential notice to Class Members of this class action can be accomplished via United States mail to all individuals who received a copy of the three Data Breach notice letters and/or through electronic mail and/or through publication.

ANSWER: The allegations in Paragraph 74 consist of legal conclusions and Plaintiffs' characterizations of their claims and terminology to which no response is required. To the extent that a further response to the allegations contained in Paragraph 74 is required, SGR denies same, denies that it is appropriate for Plaintiffs to bring claims on behalf of the purported Nationwide, California, and Georgia Classes, and denies that such classes may be certified under Rule 23 of the Federal Rules of Civil Procedure.

75. Class certification is also appropriate under Fed. R. Civ. P. 23(a) and (b)(2) because SGR has acted or refused to act on grounds generally applicable to the class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the class as a whole.

ANSWER: The allegations in Paragraph 75 consist of legal conclusions to which no response is required. To the extent that a further response to the allegations contained in Paragraph 75 is required, SGR denies the same, denies that it is appropriate for Plaintiffs to bring claims on behalf of the purported Nationwide, California, and Georgia Classes, and denies that such classes may be certified under Rule 23 of the Federal Rules of Civil Procedure.

76. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of the matters and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether SGR owed a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, processing, using, and safeguarding their personal information;

b. Whether SGR breached that legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, processing, using, and safeguarding their personal information;

c. Whether SGR failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether SGR failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the personal information compromised in the breach; and

e. Whether Class Members are entitled to actual damages, credit monitoring, injunctive relief, statutory damages, and/or punitive damages as a result of SGR's wrongful conduct as alleged herein.

ANSWER: The allegations in Paragraph 76 consist of legal conclusions and Plaintiffs' characterizations of their claims and terminology to which no response is required. To the extent that a further response to the allegations contained in Paragraph 76 is required, SGR denies same, denies that it is appropriate for Plaintiffs to bring claims on behalf of the purported Nationwide, California, and Georgia Classes, and denies that such classes may be certified under Rule 23 of the Federal Rules of Civil Procedure.

FIRST CAUSE OF ACTION
(Negligence, By Plaintiffs and the Nationwide Class Against SGR)

77. Plaintiffs reallege and incorporate by reference the preceding paragraphs as if fully set forth herein.

ANSWER: SGR realleges and incorporates by reference its preceding answers as if fully set forth herein.

78. SGR owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, storing, using, processing, deleting and safeguarding their personal information in its possession from being compromised, stolen, accessed, and/or misused by unauthorized persons. That duty includes a duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the personal information that were compliant with and/or better than industry-standard practices. SGR's duties included a duty to design, maintain, and test its security systems to ensure that Plaintiffs' and Class Members' personal information was adequately secured and protected, to implement processes that would detect a breach of its security system in a timely manner, to timely act upon warnings and alerts, including those generated by its own security systems regarding

intrusions to its networks, and to promptly, properly, and fully notify its clients, Plaintiffs, and Class Members of any data breach.

ANSWER: SGR denies the allegations contained within Paragraph 78.

79. SGR's duties to use reasonable care arose from several sources, including but not limited to those described below.

ANSWER: SGR denies the allegations contained within Paragraph 79.

80. SGR had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices. In fact, not only was it foreseeable that Plaintiffs and Class Members would be harmed by the failure to protect their personal information because hackers routinely attempt to steal such information and use it for nefarious purposes, but SGR also knew that it was more likely than not Plaintiff and other Class Members would be harmed.

ANSWER: SGR denies the allegations contained within Paragraph 80.

81. SGR's duty also arose under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect personal information by companies such as SGR.

ANSWER: SGR denies the allegations contained within Paragraph 81.

82. Various FTC publications and data security breach orders further form the basis of SGR's duty. According to the FTC, the need for data security should be factored into all business decision making.[19] In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which

[19] *Start with Security, A Guide for Business*, FTC (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf

established guidelines for fundamental data security principles and practices for business.[20] Among other things, the guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach. Additionally, the FTC recommends that companies limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures. The FBI has also issued guidance on best practices with respect to data security that also form the basis of SGR's duty of care, as described above.[21]

ANSWER: SGR denies it owes any duty. SGR lacks knowledge or information sufficient to form a belief as to the truth of the remaining allegations in this paragraph and therefore denies same.

83. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' personal information, SGR assumed legal and equitable duties

[20] *Protecting Personal Information, A Guide for Business*, FTC (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf

[21] *How to Protect Your Networks from Ransomware*, FBI, https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last viewed February 3, 2023).

and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' personal information from disclosure.

ANSWER: SGR denies the allegations contained within Paragraph 83.

84. SGR also had a duty to safeguard the personal information of Plaintiffs and Class Members and to promptly notify them of a breach because of state laws and statutes that require SGR to reasonably safeguard personal information, as detailed herein, including Cal. Civ. Code § 1798.80 *et seq*.

ANSWER: SGR denies the allegations contained in Paragraph 84. Answering further, Cal. Civ. Code § 1798.80 does not apply.

85. Timely notification was required, appropriate, and necessary so that, among other things, Plaintiffs and Class Members could take appropriate measures to freeze or lock their credit profiles, cancel or change usernames or passwords on compromised accounts, monitor their account information and credit reports for fraudulent activity, contact their banks or other financial institutions that issue their credit or debit cards, obtain credit monitoring services, develop alternative timekeeping methods or other tacks to avoid untimely or inaccurate wage payments, and take other steps to mitigate or ameliorate the damages caused by SGR's misconduct.

ANSWER: SGR denies the allegations in Paragraph 85. Answering further, SGR affirmatively asserts that it did timely issue notifications related to the Incident.

86. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their personal information.

ANSWER: SGR lacks knowledge or information sufficient to form a belief as to the truth of the allegations in this paragraph and therefore denies same.

87. SGR breached the duties it owed to Plaintiffs and Class Members described above and thus was negligent. SGR breached these duties by, among other

things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the personal information of Plaintiffs and Class Members; (b) prevent the breach; (c) timely detect the breach; (d) maintain security systems consistent with industry; (e) timely disclose that Plaintiffs' and Class Members' personal information in SGR's possession had been or was reasonably believed to have been stolen or compromised; (f) failing to comply fully even with its own purported security practices.

ANSWER: SGR denies the allegations contained within Paragraph 87.

88. SGR knew or should have known of the risks of collecting and storing personal information and the importance of maintaining secure systems, especially in light of the increasing frequency of ransomware attacks. The sheer scope of SGR's operations further shows that SGR knew or should have known of the risks and possible harm that could result from its failure to implement and maintain reasonable security measures. On information and belief, this is but one of the several vulnerabilities that plagued SGR's systems and led to the data breach.

ANSWER: SGR denies the allegations contained within Paragraph 88.

89. Through SGR's acts and omissions described in this complaint, including SGR's failure to provide adequate security and its failure to protect the personal information of Plaintiffs and Class Members from being foreseeably captured, accessed, exfiltrated, stolen, disclosed, accessed, and misused, SGR unlawfully breached their duty to use reasonable care to adequately protect and secure Plaintiffs' and Class Members' personal information.

ANSWER: SGR denies the allegations contained within Paragraph 89.

90. SGR further failed to timely and accurately disclose to clients, Plaintiffs, and Class Members that their personal information had been improperly acquired or accessed and/or was available for sale to criminals on the dark web. In fact, SGR inextricably waited more than 17 months to notify the majority of

impacted individuals of the breach. Plaintiffs and Class Members could have taken action to protect their personal information if they were provided timely notice.

ANSWER: SGR denies the allegations contained within Paragraph 90.

91. But for SGR's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, their personal information would not have been compromised.

ANSWER: SGR denies the allegations contained within Paragraph 91.

92. Plaintiffs and Class Members relied on SGR to keep their personal information confidential and securely maintained, and to use this information for business purposes only, and to make only authorized disclosures of this information.

ANSWER: SGR lacks knowledge or information sufficient to form a belief as to the truth of the allegations in this paragraph and therefore denies same.

93. As a direct and proximate result of SGR's negligence, Plaintiffs and Class Members have been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial. As a result of SGR's failure to protect Plaintiffs' and Class Members' personal information, Plaintiffs' and Class Members' personal information has been accessed by malicious cybercriminals. Plaintiffs 'and the Class Members' injuries include:

a. theft of their personal information;

b. costs associated with requested credit freezes;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. costs associated with purchasing credit monitoring and identity theft protection services;

e. unauthorized charges and loss of use of and access to their financial account funds and costs associated with the inability to

obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;

f. lowered credit scores resulting from credit inquiries following fraudulent activities;

g. costs associated with time spent and loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the data breach, including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

h. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their personal information being placed in the hands of criminals;

i. damages to and diminution of value of their personal information entrusted, directly or indirectly, to SGR with the mutual understanding that SGR would safeguard Plaintiffs' and the Class Members' data against theft and not allow access and misuse of their data by others;

j. continued risk of exposure to hackers and thieves of their personal information, which remains in SGR's possession and is subject to further breaches so long as SGR fails to undertake appropriate and adequate measures to protect Plaintiff and Class Members, along with damages stemming from the stress, fear,

and anxiety of an increased risk of identity theft and fraud stemming from the breach;

k. loss of the inherent value of their personal information;

l. the loss of the opportunity to determine for themselves how their personal information is used; and

m. other significant additional risk of identity theft, financial fraud, and other identity-related fraud in the indefinite future.

ANSWER: SGR denies the allegations contained within Paragraph 93.

94. In connection with the conduct descried above, SGR acted wantonly, recklessly, and with complete disregard for the consequences Plaintiffs and Class Members would suffer if their highly sensitive and confidential personal information, including but not limited to name, company name, address, social security numbers, and banking and credit card information, was access by unauthorized third parties.

ANSWER: SGR denies the allegations contained within Paragraph 94.

SECOND – FIFTH CAUSES OF ACTION

No response to Counts Two through Five, Paragraphs 95 through 133, is required as this Court dismissed Counts Two through Five on May 30, 2024. ECF 37.

SIXTH CAUSE OF ACTION

(Violation of the California Unfair Competition Law, Cal. Bus. & Prof. Code §17200 *et seq*.
By Plaintiff Owens and the California Subclass Against SGR)

134. Plaintiff Owens realleges and incorporates by reference the preceding paragraphs as though fully set forth herein.

ANSWER: SGR realleges and incorporates by reference its preceding answers as if fully set forth herein.

135. SGR is a "person" defined by Cal. Bus. & Prof. Code § 17201.

ANSWER: SGR admits the allegations contained in Paragraph 135.

136. SGR violated Cal. Bus. & Prof. Code § 17200 *et seq*. ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

ANSWER: SGR denies the allegations contained in Paragraph 136.

137. SGR's "unfair" acts and practices include:

a. SGR failed to implement and maintain reasonable security measures to protect Plaintiff's and California Subclass Members' personal information from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the SGR data breach. SGR failed to identify foreseeable security risks, remediate identified security risks, and adequately improve security following previous cybersecurity incidents and known coding vulnerabilities in the industry;

b. SGR's failure to implement and maintain reasonable security measures also was contrary to legislatively-declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act (15 U.S.C. § 45), California's Customer Records Act (Cal. Civ. Code § 1798.80 *et seq*.), and California's Consumer Privacy Act (Cal. Civ. Code § 1798.150);

c. SGR's failure to implement and maintain reasonable security measures also led to substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of SGR's inadequate security, consumers could not have reasonably avoided the harms that SGR caused; and

d. Engaging in unlawful business practices by violating Cal. Civ. Code § 1798.82.

ANSWER: SGR denies the allegations contained in Paragraph 137.

138. SGR has engaged in "unlawful" business practices by violating multiple laws, including California's Consumer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification), California's Consumer Privacy Act, Cal. Civ. Code § 1798.150, California's Consumers Legal Remedies Act, Cal. Civ. Code §§ 1780, *et seq*., the FTC Act, 15 U.S.C. § 45, and California common law.

ANSWER: SGR denies the allegations contained in Paragraph 138.

139. SGR's unlawful, unfair, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and California Subclass Members' personal information, which was a direct and proximate cause of the SGR data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the SGR data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and California Subclass Members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45, California's Customer Records Act, Cal. Civ. Code §§ 1798.80 *et seq*., and California's Consumer Privacy Act, Cal. Civ. Code § 1798.150, which was a direct and proximate cause of the SGR data breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and California Subclass Members' personal information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and California Subclass Members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45, California's Customer Records Act, Cal. Civ. Code §§ 1798.80, *et seq*., and California's Consumer Privacy Act, Cal. Civ. Code § 1798.150;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and California Subclass Members' personal information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and California Subclass Members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45, California's Customer Records Act, Cal. Civ. Code §§ 1798.80, *et seq*., and California's Consumer Privacy Act, Cal. Civ. Code § 1798.150.

ANSWER: SGR denies the allegations contained in Paragraph 139.

140. SGR's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of SGR's data security and ability to protect the confidentiality of consumers' personal information.

ANSWER: SGR denies the allegations contained in Paragraph 140.

141. As a direct and proximate result of SGR's unfair, unlawful, and fraudulent acts and practices, Plaintiff and California Subclass Members' were injured and lost money or property, which would not have occurred but for the unfair and deceptive acts, practices, and omissions alleged herein, monetary damages from fraud and identity theft, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their personal information.

ANSWER: SGR denies the allegations contained in Paragraph 141.

142. SGR's violations were, and are, willful, deceptive, unfair, and unconscionable.

ANSWER: SGR denies the allegations contained in Paragraph 142.

143. Plaintiff and Class Members have lost money and property as a result of SGR's conduct in violation of the UCL, as stated herein and above.

ANSWER: SGR denies the allegations contained in Paragraph 143.

144. By deceptively storing, collecting, and disclosing their personal information, SGR has taken money or property form Plaintiff and Class Members.

ANSWER: SGR denies the allegations contained in Paragraph 144.

145. SGR acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiff's and California Subclass members' rights. Past data breaches put it on notice that its security and privacy protections were inadequate.

ANSWER: SGR denies the allegations contained in Paragraph 145.

146. Plaintiff and California Subclass Members' [*sic*] seek all monetary and nonmonetary relief allowed by law, including restitution of all profits stemming from SGR's unfair, unlawful, and fraudulent business practices or use of their personal information; declaratory relief; reasonable attorneys' fees and costs under

California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief, including public injunctive relief.

ANSWER: Paragraph 146 does not contain allegations that require an answer. To the extent that a further answer is required, SGR denies the allegations contained in Paragraph 146.

SEVENTH CAUSE OF ACTION
(Invasion of Privacy)
(Count 1 – Common Law Invasion of Privacy – Intrusion Upon Seclusion By Plaintiffs and the Nationwide Class Against SGR)

147. Plaintiffs reallege and incorporate by reference the preceding paragraphs as though fully set forth herein.

ANSWER: SGR realleges and incorporates by reference its preceding answers as if fully set forth herein.

148. To assert claims for intrusion upon seclusion, one must plead (1) that the defendant intentionally intruded into a matter as to which plaintiff had a reasonable expectation of privacy; and (2) that the intrusion was highly offensive to a reasonable person.

ANSWER: Paragraph 148 contains a legal conclusion to which no answer is required. To the extent an answer is required, SGR admits that Paragraph 148 states the elements to plead an intrusion upon seclusion action.

149. SGR intentionally intruded upon the solitude, seclusion and private affairs of Plaintiffs and Class Members by intentionally configuring their systems in such a way that left them vulnerable to malware/ransomware attack, thus permitting unauthorized access to their systems, which compromised Plaintiffs' and Class Members' personal information. Only SGR had control over its systems.

ANSWER: SGR denies the allegations in Paragraph 149.

150. SGR's conduct is especially egregious and offensive as they failed to have adequate security measures in place to prevent, track, or detect in a timely fashion unauthorized access to Plaintiffs' and Class Members' personal information.

ANSWER: SGR denies the allegations in Paragraph 150.

151. At all times, SGR was aware that Plaintiffs' and Class Members' personal information in their possession contained highly sensitive and confidential personal information.

ANSWER: SGR admits the allegations contained in Paragraph 151.

152. Plaintiffs and Class Members have a reasonable expectation of privacy in their personal information, which also contains highly sensitive medical information.

ANSWER: SGR denies the allegations contained in Paragraph 152.

153. SGR intentionally configured their systems in such a way that stored Plaintiffs' and Class Members' personal information to be left vulnerable to malware/ransomware attack without regard for Plaintiffs' and Class Members' privacy interests.

ANSWER: SGR denies the allegations in Paragraph 153.

154. The disclosure of the sensitive and confidential personal information of thousands of consumers, was highly offensive to Plaintiffs and Class Members because it violated expectations of privacy that have been established by general social norms, including by granting access to information and data that is private and would not otherwise be disclosed.

ANSWER: SGR denies the allegations in Paragraph 154.

155. SGR's conduct would be highly offensive to a reasonable person in that it violated statutory and regulatory protections designed to protect highly sensitive information, in addition to social norms. SGR's conduct would be especially egregious to a reasonable person as SGR publicly disclosed Plaintiffs' and Class Members' sensitive and confidential personal information without their consent, to an "unauthorized person," i.e., hackers.

ANSWER: SGR denies the allegations in Paragraph 154.

156. As a result of SGR's actions, Plaintiffs and Class Members have suffered harm and injury, including but not limited to an invasion of their privacy rights.

ANSWER: SGR denies the allegations in Paragraph 156.

157. Plaintiff and Class Members have been damaged as a direct and proximate result of SGR's intrusion upon seclusion and are entitled to just compensation.

ANSWER: SGR denies the allegations in Paragraph 157.

158. Plaintiff and Class Members are entitled to appropriate relief, including compensatory damages for the harm to their privacy, loss of valuable rights and protections, and heightened stress, fear, anxiety and risk of future invasions of privacy.

ANSWER: SGR denies the allegations in Paragraph 158.

(Count 2 –Invasion of Privacy – Cal. Const. Art. 1, § 1 By Plaintiff Owens and the California Subclass Against SGR)

159. Plaintiff Owens realleges and incorporates by reference the preceding paragraphs as though fully set forth herein.

ANSWER: SGR realleges and incorporates by reference its preceding answers as if fully set forth herein.

160. Art. I, § 1 of the California Constitution provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." Art. I, § 1, Cal. Const.

ANSWER: Paragraph 160 does not contain allegations that require an answer. To the extent that an answer is required, SGR admits that Paragraph 160 quotes Art. I, § 1 of the California Constitution.

161. The right to privacy in California's constitution creates a private right of action against private and government entities.

ANSWER: Paragraph 161 contains a legal conclusion to which an answer is not required.

162. To state a claim for invasion of privacy under the California Constitution, a plaintiff must establish: (1) a legally protected privacy interest; (2) a reasonable expectation of privacy; and (3) an intrusion so serious in nature, scope, and actual or potential impact as to constitute an egregious breach of the social norms.

ANSWER: Paragraph 162 contains a legal conclusion to which an answer is not required. To the extent that an answer is required, SGR denies the allegations contained in Paragraph 162.

163. SGR violated Plaintiff's and Class Members' constitutional right to privacy by collecting, storing, and disclosing their personal information in which they had a legally protected privacy interest, and in which they had a reasonable expectation of privacy in, in a manner that was highly offensive to Plaintiff and Class Members, would be highly offensive to a reasonable person, and was an egregious violation of social norms.

ANSWER: SGR denies the allegations contained in Paragraph 163.

164. SGR has intruded upon Plaintiff's and Class Members' legally protected privacy interests, including interests in precluding the dissemination or misuse of their confidential personal information.

ANSWER: SGR denies the allegations contained in Paragraph 164.

165. SGR's actions constituted a serious invasion of privacy that would be highly offensive to a reasonable person in that: (i) the invasion occurred within a zone of privacy protected by the California Constitution, namely the misuse of information gathered for an improper purpose; and (ii) the invasion deprived Plaintiff and Class Members of the ability to control the circulation of their personal information, which is considered fundamental to the right to privacy.

ANSWER: SGR denies the allegations contained in Paragraph 165.

166. Plaintiff and Class Members had a reasonable expectation of privacy in that: (i) SGR's invasion of privacy occurred as a result of SGR's security practices including the collecting, storage, and unauthorized disclosure of consumers' personal information; (ii) Plaintiff and Class Members did not consent or otherwise authorize SGR to disclosure their personal information; and (iii) Plaintiff and Class Members could not reasonably expect SGR would commit acts in violation of laws protecting privacy.

ANSWER: SGR denies the allegations contained in Paragraph 166.

167. As a result of SGR's actions, Plaintiff and Class Members have been damaged as a direct and proximate result of SGR's invasion of their privacy and are entitled to just compensation.

ANSWER: SGR denies the allegations contained in Paragraph 167.

168. Plaintiff and Class Members suffered actual and concrete injury as a result of SGR's violations of their privacy interests. Plaintiff and Class Members are entitled to appropriate relief, including damages to compensate them for the harm to their privacy interests, loss of valuable rights and protections, heightened stress, fear, anxiety, and risk of future invasions of privacy, and the mental and emotional distress and harm to human dignity interests caused by Defendant's invasions.

ANSWER: SGR denies the allegations contained in Paragraph 168.

169. Plaintiff and Class Members seek appropriate relief for that injury, including but not limited to damages that will reasonably compensate Plaintiff and Class Members for the harm to their privacy interests as well as disgorgement of profits made by SGR as a result of its intrusions upon Plaintiff's and Class Members' privacy.

ANSWER: SGR denies the allegations contained in Paragraph 169.

EIGHTH – NINTH CAUSES OF ACTION

No response to Counts Eight and Nine, Paragraphs 170 through 182, is required as this Court dismissed Counts Eight and Nine on May 30, 2024. ECF 37.

WHEREFORE, DEFENDANT prays for relief as follows:

1. **That Plaintiffs take nothing by way of this Complaint;**
2. **That Plaintiffs' Complaint be dismissed with prejudice;**
3. **That Defendant recover its costs of suit herein; and**
4. **For such other and further relief as the Court may deem just and proper.**

AFFIRMATIVE DEFENSES

First Defense (for purposes of appeal only)

Plaintiffs lack standing under Article III of the United States Constitution.

Second Defense

The damages suffered by Plaintiffs, if any, were caused by the acts of others for whose conduct SGR was not responsible, including but potentially not limited to the criminals who perpetrated the Incident, and for those actions SGR cannot be found liable.

Third Defense

Plaintiffs' negligence claim is barred by the economic loss doctrine.

Fourth Defense

Plaintiffs' damages claims are barred to the extent they have failed to take steps to mitigate their alleged damages.

Fifth Defense

Plaintiffs' damages claims are barred to the extent any steps they may have taken to mitigate their alleged damages were unreasonable.

Sixth Defense

Plaintiffs' damages claims are barred to the extent Plaintiffs were contributorily negligent with respect to any damages they claim to have incurred.

Seventh Defense

Plaintiffs' claims may not properly be maintained as a class action under Rule 23 of the Federal Rules of Civil Procedure.

Eighth Defense (for purposes of appeal only)

Plaintiffs lack standing to bring their UCL claim because they have failed to adequately allege that they have suffered "lost money or property" under California Business & Professions Code § 17204.

RESERVATION OF RIGHTS

Defendant hereby gives notice that it intends to rely upon such other and further affirmative defenses as may become available during discovery in this action and reserve the right to amend its Answer to assert any such defenses. The pleading of a defense as an affirmative defense is not an admission or acknowledgement that Defendant bears the burden of proof on such defense, or waiver of any argument that Plaintiff bears such burden.

Dated: August 6, 2024 CLARK HILL

By: */s/ Myriah V. Jaworski*
Myriah V. Jaworski
Mason Floyd (*pro hac vice)*
Chirag H. Patel *(pro hac vice)*

Attorneys for Defendant
SMITH, GAMBRELL & RUSSELL, LLP